Byte Wars: The Impact of September 11 on Information Technology

By Edward Yourdon
Prentice Hall PTR, 2002

Reviewed by Scott Curthoys, a Counterintelligence Analyst contracted to a federal law enforcement agency and retired Army military intelligence and foreign area officer.

One of the many memories that I have of September 11th is of a radio announcer saying, "Everything has changed; our world will never be the same." While most of us do not see significant alterations in our daily lives, Edward Yourdon, in his newest book *Byte Wars: The Impact of September 11 on Information Technology*, focuses on the significant changes in the information technology (IT) field. Yourdon not only discusses changes *in* the IT field, but he proposes numerous necessary changes *to* the IT field. The difference one finds upon reading *Byte Wars: The Impact of September 11 on Information Technology* is not as subtle as it first seems.

The events of September 11th demonstrated to Americans that they were vulnerable targets not just in distant foreign locations such as U.S. embassies or military ships and facilities, but here at home. Much of this vulnerability stems from our dependence on ubiquitous interconnected information systems. The attack on the World Trade Center not only destroyed two buildings but also disrupted numerous computer systems supporting banking and finance, telecommunications, emergency response, and government operations. Those systems that provide us with our daily societal infrastructure are also vulnerable. Information systems are key components of water and electricity distribution systems, air and rail transport, commercial transactions, right down to the 911 system that brings life-saving help. A serious disruption in one area of the nation's critical infrastructure could cascade into other areas. Yourdon shares the view of many when he asserts that the attack of September 11th was not a "singular" event and that more attacks will occur. The current decade, he asserts, will be known as the "decade of security." It will challenge those who design, administer, or manage IT systems to think the unthinkable and identify and manage risks that they have never considered.

The strength of this book lies in Yourdon's attempt to make it relevant to the various layers and segments of the IT field that include the programmer, the project manager, and senior corporate executives as well as the middle manager. By dividing his chapters into sections such as techniques and technologies, paradigm shifts, and strategic implications, Yourdon clearly articulates the changes that must be embraced by IT professionals to mitigate the threat to American commerce and the national infrastructure.

The protection of the data within an IT system is now greater than the physical protection of that system's hardware. This is not as simple as protecting the data from hackers and other unwanted guests. This represents the reversal of a decade-long trend toward open, accessible data. The wealth of data on many corporate or government Web sites, including military sites, represents a real operations security concern. Information that has been viewed as benign or even necessary for corporate image may, in fact, provide a terrorist or criminal with a key piece of information. Moreover, the emergence of ever-smaller, ever-smarter devices (personal digital assistants, removable micro drives, and wireless connections) makes the physical interdiction of data removal almost impossible. IT systems are no longer appendages of the accounting department or inventory control. These systems now represent the brains that direct and control the operations of the company, agency, or organization. As such, they now require more thorough security. Yourdon's message is not to spend more money on security, but to make a priority of doing it better.

Events that disrupt our IT systems as well as our daily lives, which were once thought of as occurring only "once every 100 years," now seem to happen with dizzying regularity. In addition, the causes of these disruptions are not just accidental, but increasingly the result of malevolent design. To deal with these serious events, such as the attacks of September 11th, Yourdon advocates the development of two types of systems. Resilient systems are those that can withstand sudden, disruptive attacks without collapsing. They have slack or extra capacity built into critical parts that allow the IT system to "give" with the blow. Today's financially straitened times make emergent systems of particular interest to the commercial world, even more so to the military. These are ad-hoc, grassroots systems that cope with unanticipated and fast-moving disruptions that stymie traditional top-down systems. This is similar to the ageless military philosophy of "adapt and overcome." Yourdon's application of these characteristics to the seemingly rigid IT world does represent a change both in and to the industry.

Except for his chapters on good-enough systems and death-march projects, which seem non sequiturs to his principal theme of the impact from September 11th, Yourdon's book clearly points out the changes in the IT field as well as the changes to it resulting from the attack on the United States. Because IT systems will be at the heart of the U.S. response to terrorism, it is vital for all of us in the field of information technology or security to understand the forces at work on our critical systems.